

METHOD OF MULTIPLE ALGORITHM PROCESSING OF BIOMETRIC DATA

Cross-Reference to Related Applications

- 5 This application claims the benefit of U.S. Provisional Application 60/404,727 filed August 20, 2002.

Field of the Invention

- 10 The present invention relates to an identity verification system; and, more particularly, to a method of creating multiple biometric reference templates and biometric match templates from identifiable biometric data.

Background of the Invention

- 15 Biometrics is the automated use of physiological or behavioral characteristics to identify an individual or to verify an individual's identity. Biometric technologies such as fingerprint, facial recognition, iris recognition, voice verification, hand geometry, signature verification, keystroke dynamics, and retina scan are commonly used to identify or verify the identity of users attempting to access data on PCs and networks, enter secure facilities, register for public services, execute transactions, and confirm identifies to government
20 officials. Biometrics can complement or replace existing authentication methods such as passwords, PINs, tokens, cards, badges, manual signature verification, manual photograph verification, and challenge-response sequences based on personal information.

- 25 Biometric technology is based on the distinctive features resident in fingerprints, faces, irises, retinas, voices, signatures, hands, and other physiological and behavioral characteristics. These features, such as the ridge endings of a fingerprint, the shape and composition facial elements, the striations and furrows of an iris, and the pitch and cadence of a voice, can be associated with specific individuals with a high degree of confidence.

- 30 Biometric systems utilize algorithms to locate distinctive features in an automated fashion. The process of locating a physiological or behavioral characteristic's distinctive elements through an algorithm is known as feature extraction. Using information associated with these distinctive elements, biometric systems create what are known as biometric templates. The terms "biometric sample" and "biometric data" refer to the original,

identifiable data collected by the input device such as a fingerprint scanner, camera, or microphone. Biometric templates usually encoded such that the original biometric sample, e.g., a fingerprint or a facial image, cannot be reconstructed from the template.

Most biometric systems utilize different types of templates. Biometric templates
5 known as reference templates are generated when an individual enrolls or registers in a biometric system. Reference templates are stored in a biometric system and used as a basis of comparison (as a "reference") for future biometric verification and identification attempts.

Biometric templates known as match templates are generated when an individual
10 provides biometric data in order to be identified or verified – generically speaking, "matched" – against one or more reference templates. Match templates are compared with reference templates to determine their degree of similarity. If the degree of similarity exceeds a given threshold, the two templates are determined to be a "match"; if the degree of similarity fails to exceed a given threshold, the two templates are determined to be a
15 "non-match".

In today's biometric industry, templates stored and processed by biometric systems are unique to each vendor, and are not interoperable. Each of the hundreds of biometric vendors in the industry utilizes proprietary methods of feature extraction, template
20 generation, and template matching. This means that biometric systems are closed systems: a template generated through a given vendor's technology can only be used to verify and identify users enrolled in that vendor's system, and is incompatible with templates generated through other vendors' software.

Furthermore, many biometric systems, especially fingerprint systems, require that users utilize specific hardware devices. Not only do biometric vendors have proprietary
25 feature extraction and template generation software, but most vendors can only enroll and match users only on their own devices. This further underscores the closed nature of today's biometric systems.

In the vast majority of biometric systems, once reference or match templates are generated, the identifiable biometric data-such as the fingerprint image, facial image, or iris
30 image-is deleted, discarded, or destroyed. Since biometric matching is based on comparisons of templates, the identifiable biometric data is only retained temporarily in order to generate a template. Because templates are proprietary and cannot be reverse-

engineered to construct identifiable data, no non-proprietary biometric data remains once the original biometric information is deleted. An exception to this is biometric systems used for criminal identification, such as those maintained by federal and state law enforcement agencies. After proprietary biometric templates are generated from the high-resolution
5 fingerprint images acquired by live-scan devices, these biometric systems store identifiable fingerprint data for the purpose of manual resolution of inconclusive automated matches.

Another characteristic of today's biometric systems is that most systems attempt to match enrolled users by means of one matching algorithm as opposed to using a plurality of algorithms. Biometric algorithms are susceptible to both false non-matching, which is the
10 failure to match an authorized individual, and false matching, which is the incorrect matching of an individual. Failure to correctly render a match decision can occur when a feature extraction algorithm locates features not present in the enrollment template, or fails to correctly locate and encode genuine features. Certain biometric systems are less prone to false matching or false non-matching than others, and may be able to provide accurate
15 matching where other systems would fail. However, because match templates associated with a given system can only be used to compare against reference templates generated through that same system's algorithms, and no identifiable data is at hand to perform *ad hoc* matching, there currently exists no method of comparing a user's match attempt against more than one enrollment template. This reduces the ability of biometric systems to provide
20 accurate matching results.

The proprietary nature of feature extraction, template generation, template matching, and hardware devices, as well as the limited fashion in which identifiable biometric data is currently utilized in biometric systems, are major impediments to the long-term viability of the biometric industry. Once an entity enrolls its employees, customers, or citizens in a
25 given fingerprint system, for example, both the entity and the users are limited to using only this system. Should the entity decide to deploy a new, improved fingerprint system from another provider, all existing users must reenroll in the new system, as existing enrollment templates cannot be used. This poses major logistical challenges, because enrollment in biometric systems can be costly, time-consuming, and often requires that individuals
30 provide documentation or other proof of identity. The problem of enrolling existing users in new, improved versions of a biometric technology has not been addressed in the biometric industry.

Short of total population reenrollment, institutions that deploy biometric technologies such as fingerprint, facial recognition, iris recognition, and voice verification have no protection against device or technology obsolescence. There is effectively no way to “upgrade” from one fingerprint system to another, for example, or to replace older biometric systems of a given technology with more accurate, reliable systems. This problem extends to both biometric hardware and software. In most applications, institutions must deploy specific fingerprint hardware devices in conjunction with fingerprint software. While the hardware may be adequate for future use, the software algorithms could eventually prove to be insufficient for the company’s needs. In this case, both the hardware and the software would need to be replaced, and all users reenrolled, in order to move to an improved system. These are significant counterarguments against the deployment of biometric technology.

There are four reasons why this fundamental biometric problem has not been solved.

(1) Biometric vendors prefer to offer closed systems because these systems prevent deployers of their technology from easily moving to another vendor’s technology. In closed, template-based systems in which identifiable data is not present, deployers must reenroll all users should they decide to replace a biometric system. This is a significant impediment to larger institutions’ upgrading their biometric systems.

(2) The biometric industry has underestimated the problem of enrollment in biometric systems. Using fingerprint as an example, vendors have failed to recognize that requiring users to enroll again and again in a variety of fingerprint systems - for home, work, mobile devices, points of sale, ATMs and kiosks, and anywhere a finger-scan system might be deployed - is highly undesirable for reasons of logistics and trust. Initial enrollment and subsequent reenrollment are costly and time-consuming processes for institutions and individuals: institutions must establish and enforce enrollment policies, and users must spend time enrolling in biometric systems.

Enrollment is most valuable to individuals and institutions when it is a one-time event performed under controlled circumstances. During a supervised enrollment process, an individual’s identity can be verified with a higher degree of certainty than in remote or unsupervised enrollment. This greater degree of certainty regarding an individual’s identity during enrollment means that his or her biometric data can likely be associated with higher-value transactions or used to access more sensitive information. However, when users must enroll anew in every biometric system they encounter, supervised enrollment becomes much

less feasible. Even if additional enrollments were to be supervised, institutions cannot be totally certain that the individual who enrolled in system A is the same individual now enrolling in system B, though the supporting information and documentation they provide may appear legitimate. The likelihood of fraudulent enrollment increases, because an individual's identity must be reestablished by non-biometric means with each new enrollment.

(3) For reasons of privacy perception and data management, biometric vendors are normally hesitant to offer solutions that store, process, or transmit identifiable biometric data, preferring instead to utilize proprietary biometric templates. However, various systemic and operational protections can be implemented to significantly reduce the possibility of the misuse or compromise of identifiable biometric data. Moreover, many of the largest biometric systems in the world, including the forensic Automated Fingerprint Identification System (AFIS) technology used by federal and local jurisdictions as well as driver's license systems which utilize facial recognition technology, permanently store and utilize biometric data. From a data management perspective, identifiable biometric data occupies more space than biometric templates, but advances in throughput and device-level storage capability are rendering the biometric data management issue obsolete.

(4) In the fingerprint space, there is a fundamental bifurcation between peripheral vendors and live-scan vendors. Peripheral vendors develop proprietary biometric hardware and software for PC security, physical access, retail, and mobile applications. Live-scan vendors manufacture devices which acquire high-resolution fingerprint images for ongoing use and storage in forensic or civil ID systems. Whereas live-scan vendors are tasked with acquiring detailed fingerprint images whose resolution and size adhere to FBI and other imaging standards, most peripheral vendors acquire smaller, lower-resolution images whose suited solely for template generation within their own system.

The live-scan and peripheral markets are driven by different criteria, and bear different relations to institutions and end users. No technology has emerged capable of acting as a bridge between expensive, higher-quality live-scan devices, whose images are of sufficient quality to generate enrollments on any lower-quality device, and affordable, lower-quality peripheral devices, whose form factor and cost make them well suited for large-scale deployments.

In order to provide deployers with the flexibility to implement new technologies as they come available without discarding an enrolled user base, and in order to address the logistical and trust-related problems of enrollment in biometric systems, a new process is necessary by which individuals can be automatically enrolled and matched in a multiplicity
5 of biometric systems by means of a single piece of identifiable biometric data.

For purposes of this patent match templates includes templates used in 1:1 verification and 1:N identification. Furthermore any references to verification matches also include the process of identification matches and vice-versa.

10 Summary of the Invention

It is, therefore, a primary objective of the present invention to provide a method processing biometric information by use of multiple algorithms.

In accordance with one aspect of the present invention, there is provided a method for processing biometric information, comprising the steps of:

- 15 (a) capturing a biometric sample from a sensor;
- (b) transmitting the biometric sample from the sensor to a processing component;
- (c) processing the biometric sample by a first algorithm to yield a first template;
- (d) storing the first template with an associated record identifier in a storage component;
- (e) processing the biometric sample by a second algorithm to yield a second template;
- 20 (f) storing the second template in a storage component; and
- (g) associating the second template with the record identifier.

In accordance with another aspect of the present invention, there is provided a method for processing biometric samples to generate templates only after a request from a requesting authority identifying the type of template to be generated.

25

Brief Description of the Drawings

Figure 1 is a schematic block diagram of a template generation system in accordance with the present invention.

Figure 2 illustrates the process by which a reference profile is used to create system-specific
30 identifiable biometric images.

Figure 3 illustrates the process by which a reference profile works in conjunction with an image enhancement system to create system-specific biometric images.

Figure 4 illustrates a biometric matching process.

Figure 5 illustrates a process by which a reference biometric is retrieved from a database for the purposes of matching.

Figure 6 illustrates the process by which biometric matching takes place in the absence of a reference template.

Figure 7 illustrates a process by which a requesting authority executes matching through communication with a populated biometric database and template identifier.

Figure 8 illustrates a process by which a template request results in the creation on an on-demand reference template used for the purposes of matching.

10

Detailed Description of the Preferred Embodiments

Referring to Fig. 1, there is provided a schematic block diagram of a template generation system 107 incorporating therein a method of processing samples to generate templates for the purposes of storage, enrollment, or matching in accordance with the present invention.

15

A biometric characteristic 100 is presented to a scanning device 102, which acquires a biometric sample 101, or identifiable biometric data, in the form of an image or recording 103. The image or recording 103 is enhanced and filtered 105, and distinctive characteristics extracted and encoded 106, through a process 104 which results in the generation of a biometric template 108. The template 108 can be used to enroll or match a user or can be stored for subsequent system usage. The same identifiable biometric data 103, or an identical copy thereof, is enhanced and filtered 110, and distinctive characteristics extracted and encoded 111, through a second specific process 109, which results in the generation of a second biometric template 112. The template 112 can be used to enroll or match a user or can be stored for subsequent system usage.

20

Referring to Figure 2, in order to address the need in the marketplace for interoperability across devices, a method is presented through which a reference profile is used to generate system-specific identifiable images, which allow for automated creation of system-specific templates. This process improves on the traditional biometric acquisition method 101 by processing the enhanced image 201 through a system-specific reference profile 202, which encapsulates key characteristics of the enhanced image such as dimension, resolution, grayscale, shape, and orientation. The reference profile generates 203

25

a second identifiable image 204 from which system-specific templates can be generated for enrollment, matching, and storage in biometric systems.

Referring to Figure 3, data contained in the reference profile 302 is used to enable an image quality processor 303 and an image cropping component 304. These work in
5 conjunction 301 to produce system-specific images 305.

Referring to Figure 4, the standard biometric template matching process is leveraged wherein a reference template 401 stored on file and a match template 402 are compared through a template matching process 400. This template matching process leads to a matching result 403.

10 Referring to Figure 5, in the traditional authentication process, a biometric characteristic 501 is converted through template extraction 107 into a system-specific template 502. This template is compared 400 against a reference template stored in a template database 503 leading to a match result 504.

Referring to Figure 6, the proposed system improves on the Figure 5 process by
15 enabling authentication when the reference template is not stored in the template database 503. After system-specific match template creation 104 from the identifiable image 601, both the extracted match template and the identifiable biometric data or sample are temporarily retained 602. The reference database is queried 603 to determine the presence of a reference template from the same system as the match template created in 104. If one or
20 more reference templates from the individual providing data 601 are in the database, the standard authentication process occurs 400, 611. If the reference template is not in the database 503 then an enrollment template from a different biometric system, and associated with the individual providing data, is retrieved from the database 604. The reference profile 605 corresponding to the system whose template is on file 604 is used to process 300 the
25 identifiable biometric data initially retained 602. The resultant images 305 are used to create match templates 104 which are compared 400 against the retrieved enrollment templates 604. If the two templates match 606, then the initial match template generate through the biometric system 104 is stored 608, 609 in the database 503 as a reference template and associated with the individual providing data, thereby expanding the range of biometric
30 devices on which an individual can authenticate. The results of this successful match can be transmitted 610 such that the individual is authenticated 612 based on the legacy enrollment 604. If the templates do not match 611 the transaction reverts to an error state 607.

Referring to Fig. 7, there is provided a schematic block diagram of a template generation system 107 incorporating therein a method of processing samples to generate templates for the purposes of storage, enrollment, and matching in accordance with the present invention.

5 A biometric characteristic 100 is presented to a scanning device 102, which acquires a biometric sample 101, or identifiable biometric data, in the form of an image or recording 103. The image or recording 103 is enhanced and filtered 105, and distinctive characteristics extracted and encoded 106, through a specific process 104, which results in the generation of a biometric template 108. The template 108 can be used to enroll, verify, or identify a
10 user or can be stored for subsequent system usage. The same identifiable biometric data 103 is enhanced and filtered 110, and distinctive characteristics extracted and encoded 110, through a second specific process 109, which results in the generation of a second biometric template 112. The template 112 can be used to enroll, verify, or identify a user or can be stored for subsequent system usage.

15 The templates are stored in template database 113. A Requesting Authority 114 sends a request for a biometric match from a requesting authority along with a match template 115, wherein the request identifies a given record identifier. The template database 113 locates from a plurality of storage units a reference template associated with the record identifier compatible with the match template. A template comparison is
20 performed 116 and the result is transmitted to the Requesting Authority 114.

Referring to Figure 8, a process is presented 800 by which a biometric sample is stored for the purpose of generating system-specific templates subsequent to request(s) by an authorized authority. In this process, a biometric characteristic 100 is acquired through a scanning device 102. This sample is transmitted 801 to a biometric storage component 802.
25 At this point the biometric sample is available for usage by template requesters. A template requester 803 transmits a template request identifier along with a template algorithm ID. This template algorithm ID defines the algorithm through which a match template is to be generated for the template requester. A biometric template service 804 routes request packages in order to retrieve one or more biometric samples 805 from biometric storage
30 802. The biometric sample is transmitted along with the template algorithm ID 806 in order to retrieve the necessary system profile from the reference profile database and template generation databases 807. Once the reference profile and the template generation algorithm

are selected 808 from the system profile database 807, the sample can be processed through the Multiple Algorithm Processing sequence 809, as per Figure 3, in order to generate a compatible reference template 810. The reference template 810 can then be transmitted to the template requester for validation.